bizcommunity

Guard against cyber breaches: Equipping your organisation and employees

While tools such as ChatGPT have caught the public imagination, artificial intelligence (AI) and machine learning (ML), a branch of AI, are now important tools in industries ranging from travel and insurance to media and finance.

By Wendy Tembedza, Dario Milo, and Dumisani Ndiweni 15 Jul 2024

Image source: Maksim Kabakou – 123RF.com

However, as AI's capabilities improve, so does the danger it poses to cybersecurity, increasing incidents and attacks. According to the South African Banking Risk Information Centre, cyber breaches and attacks South Africa increased by 22% in 2023.

More specifically, occurrences of phishing, ransomware, and unlawful access to information have all increased markedly, with the number of victims making ransomware payments increasing by 20% in 2023. The exponential developments in AI technology have had a notable impact on these statistics.

Difficulty distinguishing fakes

Furthermore, the National Cyber Security Centre in the United Kingdom published a sobering assessment earlier this year. Generative AI and large language models (a subset of ML) will make it difficult for any person, regardless of their cybersecurity understanding level, to assess whether an email, password rese identity request, or social media engineering request is genuine or not.

AI and ML tools are and have been trained to understand how a person reads and responds to an email, impersonating to such a degree that responders cannot tell the difference between the person and the toc designed to mimic them.

CYBERSECURITY

R300m DPWI cyber theft the latest signs of failing state IT infrastructure

Lindsey Schutters 10 Jul 2024

Employer considerations associated with AI and employee data system access

As an employer, cybersecurity risk primarily lives with negligent and intentional employees who either mak judgment errors or intentionally subvert an organisation's cybersecurity policies and procedures.

In cases where an employee is suspected of aiding or abetting a cybersecurity breach, they can be suspended ahead of the associated investigation. The suspension ought to be precautionary in nature and not punitive. There is no longer a legal requirement for an employer to afford an employee an opportunity t provide reasons as to why the employee should not be suspended; the employer may proceed with the suspension without obtaining reasons from the employee.

Following suspension, and if an investigation yields a finding that *prima facie* evidence exists of fraud, a disciplinary inquiry can be initiated with dismissal as a possible outcome. Given current international trends South Africa will likely soon see class action lawsuits due to data breaches, making data policy and cybersecurity matters of existential importance to any organisation that handles large volumes of consume data.

Advice for corporates to strengthen internal cybersecurity

Organisations can take several steps to prevent data breaches or reduce their exposure to cybersecurity risks.

As a first step, organisations should do their utmost to understand where key vulnerabilities exist. Typically these are:

- Employees using weak passwords on their personal and work devices. Furthermore, employees who make password information publicly available to a passerby, such as an external service provider, by sticking a note on a monitor screen for ease of memory.
- Employees sharing their passwords with each other due to interdependencies or availability challenge
- Improper handling of password-protected work devices, such as allowing family members or external associates to use them for non-work purposes.
- Phishing, which arises as much from employee error as it does from an organisation failing to update security protocols and cyber security software.
- Employees regularly neglecting to update their devices. Updates are a vital defence of any IT infrastructure since they have the latest best practices built into them.

SMES

5 ways your small business can strengthen its cybersecurity defence

Clement Sibiya 26 Apr 2024

Beyond the above preventative measures, organisations need to prioritise regular employee cybersecurity

training and cybersecurity itself. Cybersecurity training should be mandatory and held regularly. Materials associated with cybersecurity best practices should be made easily accessible to employees.

Proactive cybersecurity management must involve and be championed by an organisation's upper management. Organisational leaders have outsized influence over employees' ability to absorb training an best practices when directed. In addition, cybersecurity training has to be mandatory during the recruitmer and employee onboarding process.

In our experience, some employers have gone as far as providing cybersecurity training to potential hires before contract finalisation and then making the new employee do it a second time as part of their inductio Others run drills and simulations of cybersecurity threats so that their teams understand what decisions should be made in situations where speed is vital.

Given the speed of AI development, employers are advised to codify data breaches or negligence relatin to a data breach as misconduct within their disciplinary codes. Policies that govern IT use within an organisation should also be constantly updated to match as best as possible developments within the cyb security landscape.

ABOUT THE AUTHOR

Wendy Tembedza, partner, Dario Milo, partner and Dumisani Ndiweni, partner, Webber Wentzel